Procura della Repubblica presso il Tribunale di Firenze

Decreto n. 55/2026 Firenze, 24 giugno 2026

Oggetto: Documento afferente all'applicazione delle disposizioni relative al trattamento dei dati personali. Nomina dei Responsabili ed Incaricati del trattamento dati personali.

Il Procuratore della Repubblica

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR);

visto il d.lgs. 18 maggio 2018, n. 51, recante «Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione ditali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio»;

visto il d.lgs. 30 giugno 2003, n. 196, *recante «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»*, come modificato dal d.lgs. 10 agosto 2018, n. 101, recante *«Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»*;

visto il Decreto Ministeriale contenente "*Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia*", nonché in materia di registri di cancelleria (DM 27 aprile 2009);

visto il decreto del Ministro della Giustizia del 4 settembre 2025 con il quale è stata nominata la responsabile della protezione dei dati nella persona della dottoressa Maria Teresa Romita;

richiamati, in particolare, l'art. 23 e l'art. 37, par. 1, lett. A del Regolamento e l'art. 2*duodecies* (Limitazioni per ragioni di giustizia) introdotto dal d.lgs. n. 101/2018 a modifica del codice in materia di protezione dei dati personali (d.lgs. n. 196/2003) in merito alla distinzione tra attività giurisdizionale e trattamento dei dati giudiziari, operati dagli uffici, non effettuati nell'esercizio di funzioni giurisdizionali;
visti i provvedimenti vigenti in questo Ufficio di Procura in materia di trattamento dei dati personali;
ritenuta l'esigenza di porre in essere degli interventi organizzativi anche al fine di aggiornare gli atti dell'Ufficio in ordine all'individuazione delle figure di riferimento previste dalla normativa, apparendo congruo e possibile procedere all'individuazione delle *«persone fisiche espressamente designate»*, come richiesto dalla legge;
ritenuto che, in linea preliminare, va premesso e ribadito che l'utilizzo dei dati personali nell'ambito dell'attività giurisdizionale in senso proprio non deve eccedere le previsioni processuali e la funzione alla stessa connessa, sicché tutte le figure operanti all'interno dell'Ufficio (magistrati, personale amministrativo e di polizia, tirocinanti, etc.) nel trattamento degli stessi devono attenersi ai limiti della normativa e delle direttive di seguito indicate e alle disposizioni di legge, astenendosi da un utilizzo non rispondente alle finalità proprie dell'attività istituzionale e dei servizi;

in qualità di "Titolare" del trattamento dei dati per la Procura della Repubblica presso il Tribunale di Firenze, ai sensi e per gli effetti del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, e del Codice della Privacy e succ. mod.,

emana la seguente

DIRETTIVA

a) Soggetti

Premesso che la Procura della Repubblica è titolare del trattamento dei dati relativi ai procedimenti giudiziari, fatte salve le competenze del Ministero della Giustizia per il trattamento dei dati amministrativi, anche relativi al personale di magistratura, e rilevato che la figura del Responsabile della protezione dei dati (RPD) è individuata a cura del Ministero della Giustizia (da ultimo con decreto del 4 settembre 2025),

DESIGNA

allo svolgimento dei compiti e delle funzioni in materia di trattamento dati, nei limiti che seguono e in relazione alle attività svolte secondo le proprie attribuzioni i seguenti soggetti:
- **il Dirigente Amministrativo**, attualmente nella persona della dottoressa Francesca Merlini, quale Responsabile del trattamento, con il compito di sovrintendere e vigilare sul rispetto da parte del personale amministrativo della normativa in materia di trattamento dati ed impartire le necessarie indicazioni;

- **i Procuratori aggiunti**, quali Sub - Responsabili del trattamento, con il compito di sovrintendere e vigilare sul rispetto della normativa in materia di trattamento dei dati relativi al Servizio, all'Ufficio o, comunque, agli affari di competenza inerenti alla propria funzione organizzativa ed impartire le necessarie indicazioni ai magistrati;
- **i Direttori/Funzionari**, quali Sub - Responsabili del trattamento, individuati come di seguito, nei provvedimenti organizzativi/ordini di servizio dell'Ufficio quali responsabili delle Unità Organizzative, degli Uffici, Sezioni, Servizi, con il compito: di sovrintendere e vigilare sul rispetto da parte degli addetti all'Ufficio della normativa in materia di trattamento dati e delle disposizioni di sicurezza; di curare il corretto utilizzo degli applicativi informatici e degli archivi cartacei nell'ambito dei rispettivi uffici e il trattamento secondo correttezza, con raccolta e registrazione di dati esclusivamente per gli scopi inerenti all'attività svolta; di adattare, eventualmente, le relative prescrizioni alle particolari esigenze degli uffici in conformità alle indicazioni ricevute.

In particolare, attualmente:

- dott.ssa Susanna Negizzi: Unità Organizzativa gestione del personale, beni e servizi;
- dott.ssa Mila Donato di Paola: Unità Organizzativa Dibattimento;
- dott.ssa Emilia Sgambelluri: Unità Organizzativa Registro Generale e Segreteria del Procuratore e DDA;
- dott.ssa Maria Teresa Nuvoli: Unità Organizzativa Casellario Giudiziale;
- dott.ssa Chiara Pozzolini: Unità Organizzativa Spese di Giustizia;
- dott.ssa Tiziana Eusepi: Unità Organizzativa Segreteria Civile;
- dott. Giampiero Manetti: Unità Organizzativa Coordinamento segreterie dei Magistrati;
- dott. Fabio Vadi: Unità Organizzativa Funzionario delegato;
- dott.ssa Elena Mucci: Unità Organizzativa SDAS e Unità Organizzativa 415 bis-408 c.p.p.
- dott.ssa Lucia Bandinelli: Unità Organizzativa e Esecuzioni penali e Cooperazione internazionale.

Sono autorizzati al trattamento dati - da effettuare secondo le disposizioni normative e di prassi, oltre che secondo le indicazioni dei soggetti sopra designati - tutti i dipendenti, il personale dì magistratura, i V.P.O., il personale amministrativo in servizio presso questa Procura della Repubblica, anche in posizione di assegnazione, comando o distacco da altri uffici o corpi dell'Amministrazione, nonché i tirocinanti, gli stagisti e gli altri collaboratori legittimamente abilitati (es. polizia giudiziaria), in relazione agli affari, alle mansioni e ai compiti a ciascuno assegnati.

Sono autorizzati al trattamento dei dati per i sistemi civili i soggetti indicati nell'allegato A) e per i sistemi penali i soggetti indicati nell'allegato B) per le attività e con i limiti ivi elencati.

In particolare: deve essere osservato il corretto utilizzo degli applicativi informatici e degli archivi cartacei; il trattamento va svolto secondo correttezza, con raccolta e registrazione di dati esclusivamente per gli scopi inerenti all'attività svolta; i dati vanno conservati in conformità alle misure di sicurezza, garantendo in ogni operazione di trattamento - sia cartaceo sia automatizzato -

la massima riservatezza, evitando l'accesso da parte di terzi, anche se dipendenti dell'amministrazione e, quindi, in caso di allontanamento anche temporaneo dal posto di lavoro, ogni incaricato e autorizzato al trattamento deve accertarsi che non sia possibile l'accesso ai dati da parte di terzi, anche se dipendenti.

b) Dati trattati e modalità di trattamento

Presso la Procura della Repubblica si trattano dati del personale amministrativo e di magistratura necessari per la gestione del rapporto di lavoro e ad essa connessi, nonché dati personali, anche particolari e relativi a procedimenti giudiziari, necessari per lo svolgimento della propria funzione istituzionale.

Il personale amministrativo e di magistratura è autorizzato al trattamento dei dati strettamente necessari allo svolgimento dei propri compiti, secondo le prescrizioni normative vigenti, le direttive sopra emanate e le ulteriori specifiche indicazioni ricevute, ed è tenuto allo stesso modo a garantirne l'integrità, la correttezza e la conservazione nonché la massima riservatezza, evitando che ad essi possano accedere soggetti non autorizzati, in particolare nel caso di allontanamento dall'ufficio.

Ogni copia informatica o cartacea di documenti o dati può essere rilasciata solo a chi dimostri di avere la titolarità a ottenerla.

Nel caso si debba procedere alla distruzione (anche parziale) di dati, cartacei o informatici, anche in copia, ferme restando le competenze e la disciplina relativa alla Commissione di scarto dell'Ufficio, i Responsabili del trattamento dei dati personali devono adottare tutte le misure necessarie a evitare che i dati possano essere individuati o recuperati dopo la distruzione e che si possa riconoscere il contenuto o la provenienza del documento.

c) Misure di sicurezza relative al trattamento dati mediante apparecchiature hardware e software

L'accesso agli elaboratori in uso al personale amministrativo e di magistratura deve avvenire esclusivamente secondo i previsti profili di accesso ed è consentito sulla base di apposite autorizzazioni, rilasciate e revocate dal Procuratore della Repubblica, dai Procuratori aggiunti, dalla Dirigente Amministrativa e dai Direttori o Funzionari individuati quali responsabili degli uffici.

L'accesso agli elaboratori deve poter avvenire solo tramite l'utilizzo di credenziali personali rilasciate dall'Ufficio e di una password che va modificata con cadenza semestrale.

Gli elaboratori non devono essere mai accessibili indistintamente, ma esclusivamente secondo i previsti profili di accesso.

In caso di allontanamento dell'utente dalla postazione di lavoro l'elaboratore deve essere spento o posto in stand by. Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

Gli *account* personali sono gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso o di mancato utilizzo dei medesimi per un periodo superiore a sei mesi.

I programmi e le apparecchiature di protezione contro il rischio di intrusione o danneggiamento ad opera di terzi sono gestiti a livello centrale dal Ministero della Giustizia.
L'accesso ai programmi e alle banche dati di pertinenza esclusiva dell'Ufficio è consentito sulla base di autorizzazioni rilasciate e revocate dal Procuratore della Repubblica o suo delegato.
L'autorizzazione all'accesso deve in ogni caso intendersi limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento.

d) Misure di sicurezza relative al trattamento dati contenuti in documentazione e archivi cartacei

I fascicoli dei procedimenti sono conservati all'interno delle segreterie in armadi chiusi e in zone non accessibili al pubblico.
I fascicoli sottoposti a frequenti movimentazioni non devono recare in copertina indicazioni che permettano di risalire al soggetto cui si riferiscono.
I fascicoli, nelle fasi di trasporto all'interno dell'Ufficio, devono permanere nei corridoi il tempo strettamente necessario alla loro consegna. Il trasporto deve essere effettuato con modalità tali da garantire la riservatezza dei documenti e da impedire la visione di ogni dato a persone non autorizzate.
I fascicoli devono essere conservati e custoditi con cura e restituiti al termine delle operazioni necessarie.
Gli incaricati e autorizzati al trattamento devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati e i fascicoli agli stessi affidati devono essere conservati e custoditi con cura e restituiti al termine delle operazioni necessarie. Nessuno può accedere ad un archivio se non è autorizzato.
Gli atti e i documenti che contengano dati sensibili o dati particolari, i fascicoli personali e i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati in contenitori muniti di serratura anche da parte degli autorizzati al trattamento.
La documentazione del medico competente di cui al d.lgs. n. 81 del 2008 e qualsiasi altro documento inerente allo stato di salute o ad altri dati personali parimenti sensibili, deve essere tenuta, in busta chiusa, negli armadi in uso alla competente segreteria, chiusi con chiave custodita dal Direttore dell'Ufficio amministrativo e nell'osservanza delle prescrizioni di dettaglio impartite dal Dirigente amministrativo con appositi provvedimenti.

e) Accesso agli Uffici

L'accesso degli utenti, pubblico, avvocati e loro collaboratori presso gli uffici e le Segreterie dei Pubblici Ministeri deve avvenire esclusivamente negli orari di apertura al pubblico. L'accesso alle Segreterie da parte dei soggetti legittimati è consentito uno per volta in modo tale da garantire la riservatezza dei colloqui e delle richieste dei singoli utenti.
Il personale di vigilanza preposto agli accessi all'ufficio di Procura è tenuto a identificare il richiedente l'accesso mediante documento d'identità o tesserino dell'Ordine professionale. La

consultazione di atti di procedimenti deve avvenire sempre alla presenza del personale di segreteria competente.

In relazione a tutte le misure e le modalità di trattamento dei dati previste nel presente provvedimento, sono fatti salvi i diversi o più rigorosi presidi eventualmente necessari in conformità a specifiche previsioni legislative o regolamentari, previsti nei provvedimenti organizzativi vigenti.

Segue in allegato C) al presente provvedimento il ***MANUALE DI SICUREZZA PER GLI UTENTI.***

DISPONE

che il presente provvedimento:

-sia inoltrato a tutti i Magistrati dell'Ufficio, anche onorari, al Dirigente Amministrativo, al Personale amministrativo, ai tecnici informatici e agli appartenenti alla polizia giudiziaria in servizio presso questa Procura della Repubblica, nonché ai tirocinanti assegnati all'Ufficio, alle RSU e al medico competente;

- sia pubblicato nel sito *web* della Procura della Repubblica di Firenze, nella sezione *"Amministrazione trasparente"* unitamente al ***MANUALE DI SICUREZZA PER GLI UTENTI.***

Il Procuratore della Repubblica
Rosa Volpe

(Allegato C al decreto n. 55/2026)

Procura della Repubblica presso il Tribunale di Firenze

Manuale di sicurezza per gli utenti

La Direzione Generale per i Servizi Applicativi (già DGSIA) ha racchiuso la normativa in materia di sicurezza di trasmissione, interscambio, accesso e conservazione dei documenti informatici nel PSS (Piano strategico di sicurezza), trasmesso a tutte le articolazioni Ministeriali ed Uffici Giudiziari; questi sono tenuti a realizzare le misure proattive e reattive previste, per ridurre i rischi nel campo della sicurezza informatica e reagire agli eventuali incidenti.

I documenti informatici trattati dall'Amministrazione Giudiziaria sono comunque inerenti a un'attività fondamentale dello Stato che deve essere preservata da intromissioni esterne; devono essere trattati al fine di garantirne integrità e provenienza, disponibilità e confidenzialità (secretazione) e devono essere tutelati nell'ambito di specifici flussi di lavoro, considerandone la struttura e le specifiche tecniche di conservazione fisica, oltre che la tipologia giuridica.

Il trattamento dei dati personali, svolto da questo Ufficio nell'ambito esclusivo delle sue finalità istituzionali, con o senza ausilio degli strumenti elettronici, deve avvenire nel rispetto dei principi fissati dall'articolo 5 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali (GDPR, General Data Protection Regulation):

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione di quelli che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: è necessario provvedere alla conservazione dei dati per il tempo strettamente necessario agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Per una corretta applicazione dei principi esposti, e quindi a garanzia di un'adeguata tutela dei diritti degli interessati, è importante che i dipendenti rispettino le seguenti indicazioni, tenuto conto che l'accesso alle informazioni avviene per mezzo di sistemi informatici censiti dalla Direzione Generale per i Servizi Applicativi (già DGSIA), sulla base dei profili di autorizzazione definiti dalle mansioni assegnate:

- garantire i diritti degli interessati e comunque osservare il principio di necessità, di esattezza e aggiornamento delle informazioni trattate, nonché il principio di pertinenza;
- trattare i dati personali di cui vengono a conoscenza nello svolgimento delle proprie funzioni in modo lecito e secondo correttezza, essendone vietata la diffusione, la comunicazione e l'utilizzo oltre il dovuto;
- effettuare la raccolta, l'elaborazione, la registrazione ecc. di dati personali esclusivamente per gli scopi inerenti all'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati;
- osservare scrupolosamente tutte le misure di sicurezza già in atto, o che verranno comunicate in seguito dal Titolare/Responsabile/Sub-Responsabile del trattamento;
- assicurare la custodia dei dispositivi e la segretezza delle proprie credenziali di autenticazione;
- utilizzare password non facilmente ricostruibile dai propri dati personali, che non dovrà essere comunicata a terzi;
- cambiare la password almeno ogni sei mesi se sono trattati dati personali e ogni tre mesi quando sono trattati dati sensibili o giudiziari (su espressa autorizzazione di legge che specifichi la finalità di rilevante interesse pubblico, la tipologia dei dati trattati e le operazioni di trattamento);
- evitare di lasciare aperta una sessione di lavoro, dopo essersi identificati con il proprio login e la propria password, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- in caso di prolungata assenza o impedimento del dipendente che tratta dati personali, saranno impartite (dal direttore amministrativo responsabile dell'ufficio/cancelleria) idonee e preventive disposizioni scritte volte ad individuare le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici. In tal caso, la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della custodia delle copie, i quali informeranno tempestivamente il dipendente dopo ogni intervento effettuato con le sue credenziali;
- garantire i diritti degli interessati e comunque osservare il principio di necessità, di esattezza e aggiornamento delle informazioni trattate, nonché il principio di pertinenza;
- effettuare la raccolta, l'elaborazione, la registrazione ecc. di dati personali esclusivamente per gli scopi inerenti all'attività svolta e nei limiti strettamente necessari per adempiere ai compiti assegnati a ciascuno;
- mantenere aggiornate tutte le banche dati cui hanno accesso e non eccedere le finalità per le quali sono stati raccolti, elaborati e registrati;
- evitare di creare banche dati nuove senza espressa autorizzazione;
- conservare negli spazi e con i metodi indicati dal titolare/responsabile, tutti i documenti contenenti dati sensibili, evitando di trattenerli per un tempo superiore a quello minimo necessario per l'espletamento dei propri compiti ed in caso di interruzione anche temporanea del lavoro verificare che i dati non siano accessibili a terzi;

- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del titolare/responsabile;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al dirigente dell'ufficio responsabile per la successiva comunicazione al titolare/ responsabile del trattamento.

Di seguito i principali suggerimenti e le istruzioni per aumentare la sicurezza globale del sistema:

TRATTAMENTO DATI CON STRUMENTI ELETTRONICI
-CAUTELE GENERALI-

- ***Spegnere il computer se ci si assenta per un periodo di tempo lungo***

Un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro; più lungo è il periodo di assenza, inoltre, maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

- ***Non lasciare lavori incompiuti sullo schermo ed evitare di lasciare aperta una sessione di lavoro dopo essersi identificati***

Chiudete le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro: potreste rimanere lontani più del previsto e una postazione aperta è vulnerabile a trattamenti non autorizzati.

- ***Salvaschermo***

Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

- ***Non riutilizzare supporti rimovibili (CD, pendrive ecc..) per affidare a terzi i vostri dati***

Quando un file viene cancellato da un supporto magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai dischi. Solo l'uso di un apposito programma di cancellazione sicura garantisce che sul dischetto non resti traccia dei dati precedenti. Se ciò non è possibile, essi devono essere distrutti e comunque è sempre meglio usare un dischetto nuovo.

- ***Prestare particolare attenzione all'utilizzo dei computer portatili***

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password sui BIOS, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed effettuate periodicamente il backup.

- ***Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso***

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

- ***Proteggere il proprio computer con una password. Abilitare ove possibile l'accesso tramite password***

La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza. Non permettere l'uso del proprio computer o del proprio account da personale esterno, a meno di non essere sicuri della loro identità.

- ***Non utilizzare apparecchiature non autorizzate per cui non si è autorizzati***

L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutta la rete di cui fate parte. È quindi vietato l'uso di modem all'interno della rete locale.

- ***Non installare programmi non autorizzati***

Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

- ***Proteggere attentamente i dati***

Bisogna prestare particolare attenzione ai dati di cui si è personalmente responsabili. Come minimo bisogna posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

L'utilizzo dei dati personali deve avvenire in base al principio del "need to know": non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative. I dati non devono essere comunicati all'esterno dell'Ufficio Giudiziario e comunque a soggetti terzi se non previa autorizzazione.

- ***Usare, se possibile, il salvataggio automatico dei dati. Non dimenticare i salvataggi volontari***

Molti applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.

- ***Utilizzo del PC***

L'utente deve attenersi scrupolosamente all'utilizzo del PC solo ed esclusivamente per attività di Ufficio, ed è fatto divieto, salvo operazioni semplici (es. sostituzione di mouse o di tastiera che non possano compromettere la funzionalità del PC) assumere iniziative personali per porre rimedio ad eventuali problemi tecnici.

- ***Amministrare correttamente le password***

Con l'arruolamento delle postazioni di lavoro sul sistema nazionale ADN vengono utilizzate dei criteri e policy di sicurezza più rigidi. In particolare, se l'utente inserisce erroneamente per tre volte consecutive le proprie credenziali l'account viene bloccato per un certo lasso di tempo ed inoltre la password ha una durata 90 gg. La password deve essere periodicamente sostituita e NON può essere comunicata a terze persone.

➢ ***Non violare le leggi in materia alla sicurezza informatica.***

Ricordatevi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Non utilizzate senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.

➢ ***Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro***

Può essere il sintomo di un attacco in corso.

PRESCRIZIONI PARTICOLARMENTE IMPORTANTI -VIRUS E MISURE ANTIVIRUS-

Gli utenti devono:

- usare soltanto programmi provenienti da fonti fidate perché copie sospette di programmi possono contenere virus o altro software dannoso;
- assicurarsi di non far partire accidentalmente il computer da supporto esterno e, se possibile, impostare il BIOS in modo da avere come *primary boot device* il disco rigido e proteggere l'accesso al BIOS tramite password. Se il supporto fosse infetto, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file;
- proteggere i supporti da scrittura quando possibile. È il più efficace mezzo di prevenzione, infatti i virus non possono rimuovere la protezione meccanica;
- salvare o sottoporre a backup i dati importanti per evitare di perderli in caso di infezione.

Gli utenti non devono:

- aprire mail di provenienza sospetta e, in generale, non aprire nessun allegato senza una preventiva scansione antivirus;
- visitare siti illegali, usati come specchietto per le allodole per attirare visitatori su cui condurre attacchi;
- modificare le configurazioni del software antivirus.

POSTA ELETTRONICA

Gli utenti devono:

- Prestare la massima attenzione nella apertura dei file allegati a messaggi di posta elettronica certificata, ivi compresi quelli ricevuti mediante il protocollo documentale, perché potrebbero contenere allegati malevoli;
- usare solo il software di posta approvato dal Ministero della Giustizia;
- effettuare la scansione con programmi di controllo antivirus approvati dal Ministero dei messaggi in ingresso per evitare virus o contenuti maligni;
- impedire ad altre persone di utilizzare il proprio account per inviare posta elettronica;
- trasmettere dati confidenziali solo se adeguatamente cifrati (standard S/MIME);
- trasmettere di preferenza messaggi con firma digitale (standard 5/MIME con firma di tipo deatched), per garantire al destinatario l'origine del messaggio.

Gli utenti non devono:

- utilizzare la posta elettronica per scopi in conflitto con il piano di sicurezza ed in ogni caso non utilizzarla eccessivamente per scopi personali;
- partecipare alle cosiddette "Catene di Sant'Antonio" o, in generale, non utilizzare la posta elettronica per spamming;
- inviare mai informazioni confidenziali tramite posta elettronica non cifrata;
- aprire posta elettronica di provenienza dubbia, accertarsi sempre della provenienza dei messaggi di posta elettronica contenente allegati, nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati.

INTERNET

- Evitare l'accesso a siti in contrasto con il profilo etico specifico della nostra organizzazione o che possono costituire motivo di distrazione nell'espletamento dell'attività lavorativa;
- Salvaguardare la rete geografica da un uso eccessivo e non legato ad esigenze lavorative del servizio di navigazione Internet.

TRATTAMENTO DATI SENZA L 'AUSILIO DI STRUMENTI ELETTRONICI -CAUTELE GENERALI-

➢ ***Chiudere a chiave armadi/cassetti ed uffici***

Il primo livello di protezione di qualunque sistema è quello fisico. È certamente vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania o visibili su uno schermo. Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre, chiudete i documenti a chiave nei cassetti ogni volta che potete. I documenti contenenti dati personali non devono in alcun modo rimanere incustoditi e a fine giornata devono essere riposti in armadi /cassetti chiusi a chiave in modo da non essere accessibili a persone non autorizzate;

➢ ***Conservare supporti di memoria e stampe in luoghi sicuri***

Alla conservazione dei supporti di memoria (CD; pendrive...) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sottochiave non appena avete finito di usarli.

➢ ***Maneggiare e custodire con cura le stampe di materiale riservato***

Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo

sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più.

- ***Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali***

Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una distruggidocumenti; in ogni caso non gettate mai documenti cartacei senza averli prima sminuzzati in modo da non essere ricomponibili.

Sanzioni per inosservanza delle norme

Le presenti istruzioni integrano elementi di valutazione della condotta del lavoratore. La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della condotta.

Firenze, lì 24 giugno 2026

Il Dirigente Amministrativo
Francesca Merlini

Il Procuratore della Repubblica
Rosa Volpe